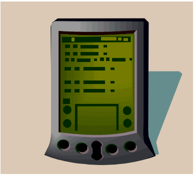
Acela Technologies, Inc.

Working Together for a More Secure IT Wireless Network

by Daryl A. Boffman
President/CEO

September 25, 2003

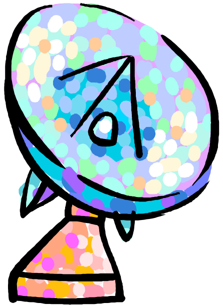
Introduction



- Cellular created an infrastructure for capacity and created public demand for more things wireless.
- Wireless networks provide mobility, speed, convenience, increased productivity and are inexpensive and easy to deploy.
- Wireless LANs sales predicted to be just under 2.5 million in 2001. Actual Sales reached $1.45 billion.
- Security is the top concern for organizations considering Wireless Networks.
- Wireless networks can be effectively secured with an adequate network security plan, multi-layered tools, and training.

Wireless Networking Basics

Wireless Communication is achieved through the following:

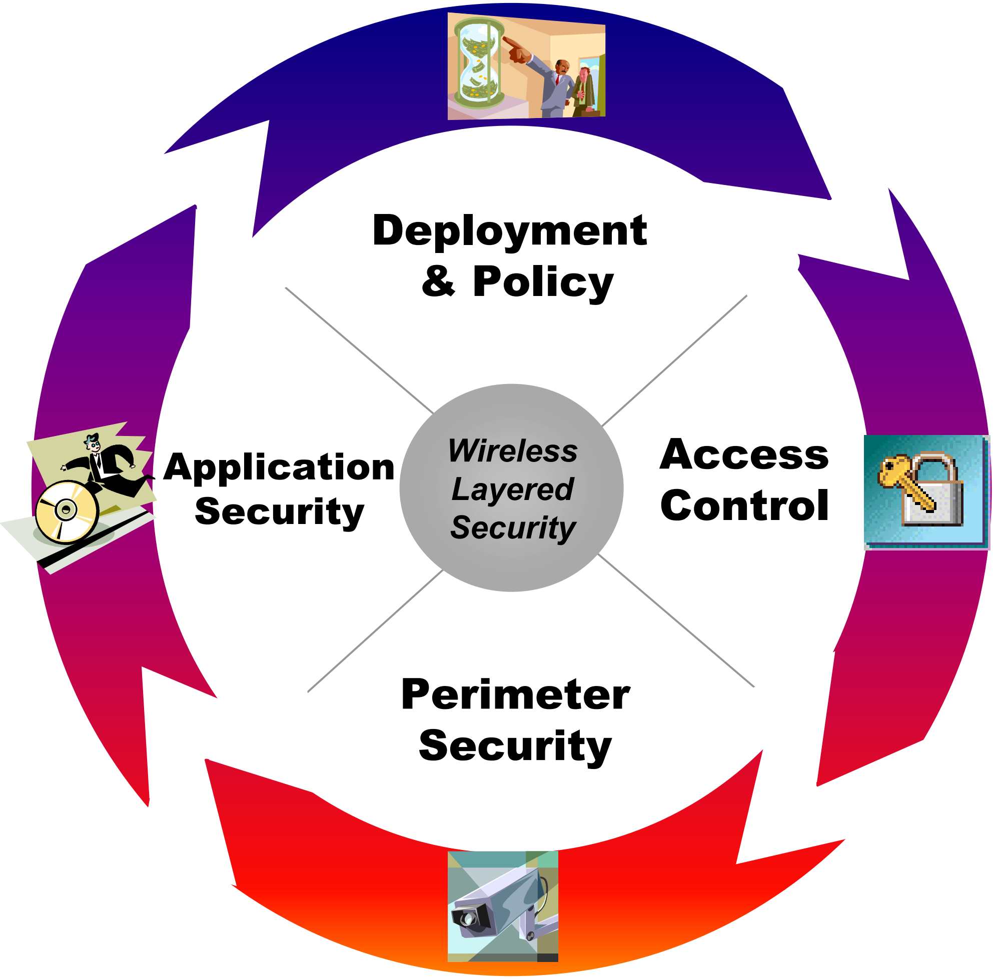


- Radio Frequency (RF)
- Wireless Access Points (WAP)
- Wireless Network Interface Cards (NIC)
- Wireless Antennas
- Wireless Devices (Laptop, PDA, etc.)
- Common Forms: Bluetooth & 802.11

Wireless Layered Security

- Layer 1. - Wireless Deployment & Policy
- Layer 2. – Wireless Access Control
- Layer 3. – Perimeter Security
- Layer 4. – Application Security

Wireless Layered Security Life-Cycle



Layer 1. Wireless Deployment & Policy

- Deploy Minimum WAPs for Coverage
- Set WAP Broadcast Power to Low
- Verify interior/exterior Broadcast Coverage
- Maintain Policies for:
  - Installation of WAPs
  - NIC Operational Mode
  - WLAN User Group Access

Layer 2. Wireless Access Control

- Configure WEP for Highest Level of Encryption
- Change SSID regularly
- Do Not Broadcast SSID
- Verify MAC Address upon Device Connection
- Maintain and Enforce Access Policies

Built-In Wireless Access Control

- Wired Equivalent Privacy (WEP) encryption – The encryption standard for wireless transmissions.
- Service Set Identifiers (SSIDs) – A shared identifier common to all the devices on a WLAN to establish contact with the WAP.

Encryption

- The Two Most Common Computer Encryption Systems:
  - Symmetric-Key Encryption – A code is shared by two computers.
  - Public-Key Encryption – A combination of a Private Key and a Public Key.

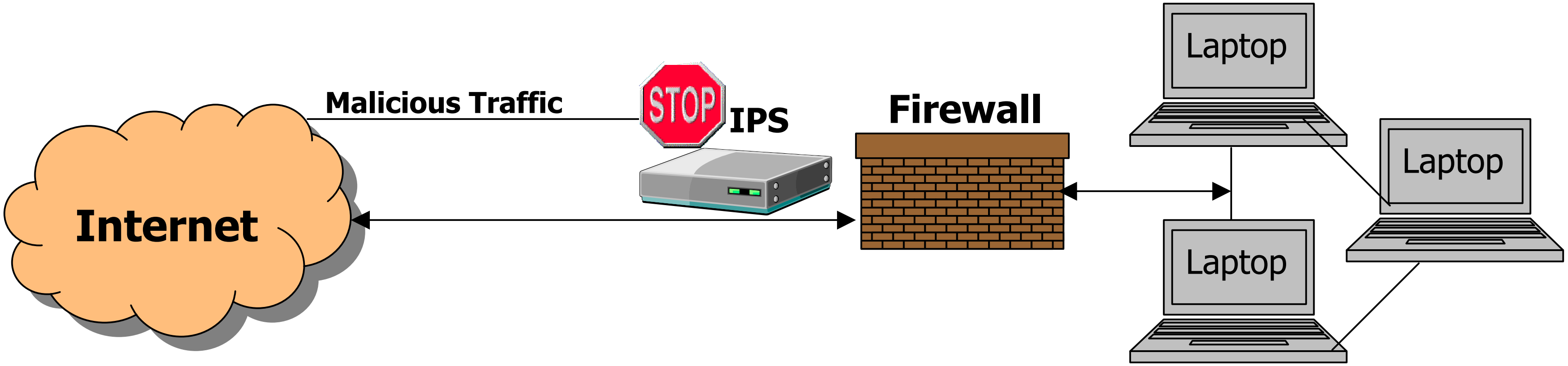
- Transport Layer Security – An Internet security protocol used by Web Browsers and Web Servers to transmit sensitive Information

Layer 3. Perimeter Security

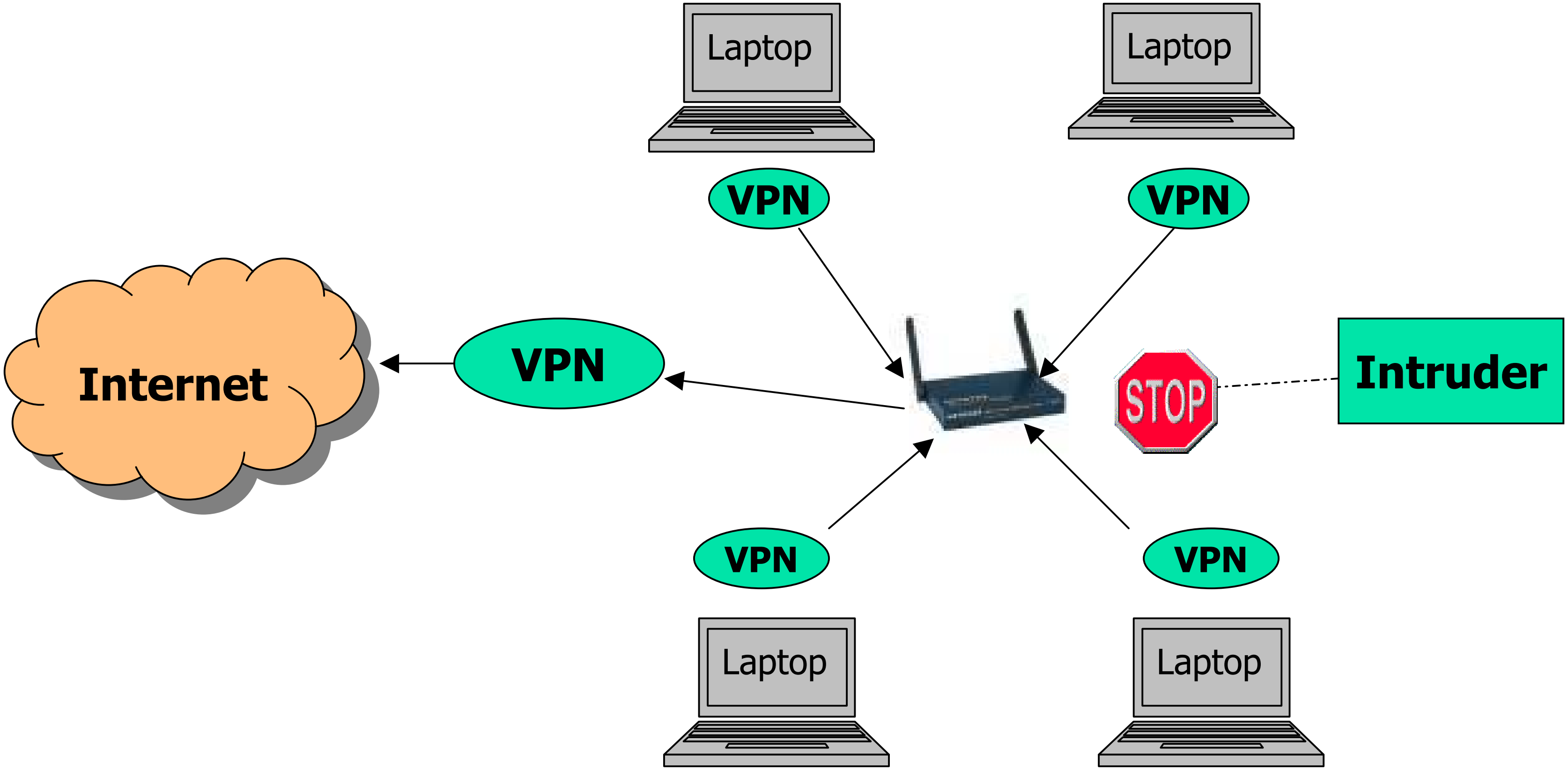
- Install Intrusion Prevention System (IPS)
- Install Wireless Firewall
- Install Anti-Virus Software
- Encrypt WLAN traffic using VPN
- Direct all Traffic through VPN Server
- Maintain and Enforce VPN Routing and Access Policies
- Maintain and Enforce User Authentication Access Policies

Perimeter Security –Firewall/IPS

- Firewall - A program or hardware device that filters information traffic flowing in and out of the network.
- IPS – Intrusion Prevention Systems block malicious attacks.



Perimeter Security – 802.11 w/VPN



Anti-Virus Tools

- Most Common Types of Infections:
  - Viruses – Piggybacks on real programs
  - E-mail Viruses – Travels on E-mail Messages
  - Worms – Travels on Networks & Security Holes
  - Trojan Horses – Damaging Computer Programs
- Anti-Virus Tools
  - Intrusion Prevention Systems
  - Vulnerability Assessment and Management
  - Anti-Virus
  - Firewalls

Layer 4. Application Security

- Implement Application-Level User-Authentication System
- Maintain and Enforce Permissions and Password Policies
- Promptly Install Vendor Patches

Network Security Lifecycle

•**Assess** – Your Plan and Current Network Security Infrastructure.

•**Invest** – In the Staff, Training, Equipment, Software and Solutions needed to achieve your Security Plan.

•**Test** – To ensure conformance to policies and standards.

•**Stress** – Management's commitment to developing and maintaining a sound Network Security Infrastructure.

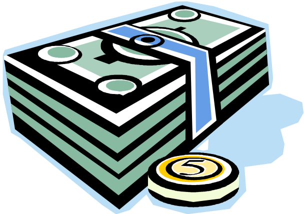
ASSESS

Network Security Assessments Focus Areas

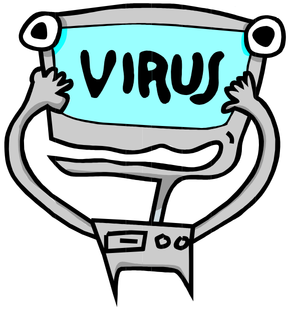
- Understanding the Mission & Environment
- Security Policies and Procedures
- Network Infrastructure
- Firewall
- Intrusion Detection
- Anti-Virus
- Host Security
- Backup/Recovery
- Application Security

INVEST

Layered Network Security Approach



- Perimeter – Firewall, Anti-Virus, VPN
- Network – IDS/IPS, VA, Access Control/User Authentication
- Host – IDS, VA, Anti-Virus, AC/UA
- Application – Application Shield, AC/UA, Input Validation
- Data – Encryption, AC/UA



TEST

Monitor, Audit and Test

- Monitor network activity for possible security vulnerabilities. Monitor Security Newsgroups.

- Audit new system installations to ensure conformance to existing policies. Audit critical files and router configurations. Perform random security audits.

- Test and install patches and fixes for security vulnerabilities in vendor software.

STRESS

Management should Develop, Maintain & ***Enforce:***

- Security Mission Statement
- Security Awareness Program
- Security Policies & Procedures
- Security Auditing and Improvement Tools
- Trained System Security Admin/Staff

STRESS, continued

7 Top Management Security Errors

1. Pretend the problem will go away
2. Authorize Reactive, Short-term Fixes
3. Fail to realize information and organizational net worth
4. Rely Primarily on Firewall for Security Protection
5. Fail to deal with Operational aspects of security
6. Lack of understanding consequences of poor information security
7. Assign untrained people to maintain security

Summary

- Wireless Technology:
  - Is here to Stay.
  - Is easy to install, increases productivity and flexibility, and is inexpensive.
  - Can provide adequate information security
  - Will continue to evolve, increasing its acceptability in the consumer, commercial, federal, and international marketplace.
  - Let’s work together for a more secure wireless IT Network.

Questions

Contact Information

- Daryl A. Boffman
  President/CEO
  Email: dboffman@acelatechnologies.com

- James (Jim) Dertzbaugh
  Vice President of Business Development
- Email: jdertzbaugh@acelatechnologies.com

- 201-A Broadway Street, 2nd Floor
  Frederick, MD 21701
- Phone (301) 846-9060
- Fax (301) 846-9062
- Website: www.acelatechnologies.com

- Thank you for your time.
- Enjoy the Conference!